Test and Evaluation: A Key Component of DoD Transformation

John P. Stenbit

Assistant Secretary of Defense (Command, Control,
Communications and Intelligence), Washington, D.C.

The Department of Defense (DoD) is committed to transformation—a transformation that, in large part, involves both the adoption of, and adaptation to, information-age technologies. In the final analysis, the success of our efforts at transformation will be directly related to our ability to bring information to bear in warfighting and other national security missions, as well as in the business processes necessary to acquire capabilities and to support operations.

As stated in a recent submission to Congress,[1] "Network Centric Warfare (NCW) is no less than the embodiment of an Information Age transformation of the DoD. It involves a new way of thinking about how we accomplish our missions, how we organize and interrelate, and how we acquire and field the systems that support us." The changes in our approach to the way we employ, acquire and field systems will pose significant challenges for the test and evaluation community.

NCW is predicated upon the ability to create and share a high level of awareness and to leverage this shared awareness to rapidly self-synchronize effects. This will allow us to apply all available information and assets to greatly increase combat power. Of course, NCW requires that we think about information differently, particularly about the way we disseminate it. Peer-to-peer relationships and information exchanges that transcend individual systems and organizations will predominate. The edge of the organization will be empowered, and command will involve choosing from a set of alternatives presented from the edge rather than from centralized planning. This, in turn, affects the attributes of information systems that are most important, and hence has profound implications for what we should test and how we should test it.

NCW involves a historic shift in the center of gravity from platforms to the network. In NCW, the single greatest contributor to combat power is the network itself. The value of platforms, headquarters and other assets derive their value, in NCW, from their ability to contribute to the overall effort by virtue of their being connected to the net. The marginal value of an unconnected platform pales in comparison to the value it can generate if it is "net ready." For example, the information generated by a networked sensor serves to enhance the value of all the other nodes on the net rather than a few nodes. Given this shift in value, the focus of test and evaluation needs to shift from the performance of individual battle-space entities to their ability to add to the value of the networked force.

As the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C^{3}I]) and the Department's chief information officer (CIO), it is my responsibility to provide the "infostructure" needed to support network-centric operations and the transformation of DoD business processes. Specifically, I am committed to:

■ Making information available on a network that people depend on and trust;

■ Populating the network with new, dynamic sources of information to defeat the enemy; and

■ Denying the enemy information advantages and exploiting weaknesses.

Toward these ends, we are working to deploy a ubiquitous, secure and robust network while eliminating limitations in bandwidth, frequency and computing capacity. To enhance the process of interpreting the available information, we are working to deploy collaborative environments and other performance support tools. At the same time, we are working to ensure that both the network and its information are secure and assured.

NCW is about the sharing of information. We are working through policies and programs to ensure that the network is populated and continuously refreshed with quality data, including intelligence, non-intelligence, raw and processed. Information not on the network has very limited value. We recognize that all users of information

John P. Stenbit

are also suppliers and that, as suppliers, they have a responsibility to post information before they use it, thereby ensuring that all the information is available to those who need it.

This move away from a "supplier push" mentality is simply a recognition of the fact that no one can possibly know everyone who can put the information to good use, appreciate the tolerance for ambiguity of others or understand how the information could be used effectively. A move from push to pull shifts the burden of finding the necessary information to the users.

Awareness, a touchstone of NCW, is not a property of a system, but rather, an attribute to be found in the cognitive domain. Measuring what information is available in a system is not an adequate measure of the level of awareness achieved. We would be remiss if we did not address the myriad issues related to the ability of the forces to make sense out of the information available on the net.

Information is not always easy to obtain. Our ability to populate the net with quality information will depend in part on our ability to develop new ways to gain access to information. We seek to surprise the enemy with the information we are using by collecting persistent, responsive, exquisite intelligence. An important aspect of the transformation involves a shift in the nature of the missions we are able to perform. For the most part, these non-traditional missions require new types of information that, in turn, involve new sources.

At the same time that we are enhancing our own information-related capabilities, we must seek to deny these advantages to others. Therefore, our ability to conduct offensive information operations is essential. As adversaries will seek to do the same to us, we must implement full-spectrum security.

In reviewing what I seek to achieve in my roles as ASD(C^3I) and the Department's CIO, it is clear that these are not properties of a system but properties of a network—a network that is dynamic in a number of dimensions. It is also clear that my efforts are not confined to the physical and information domains, but they extend to the cognitive domain as well. My focus is not on supporting individual commanders or units, but on supporting groups of distributed individuals working collaboratively.

Guest Editorial

The challenges are considerable for both of our communities. New ways are needed to instrument, analyze and evaluate federations of systems and distributed teams operating in a networked environment. Reality is the only "test environment" that will allow us to adequately test new systems along with co-evolved processes. Therefore, we will need to find ways to add and subtract systems and capabilities to the current baseline, without destroying the integrity/security of the operational system, assessing proposed increments both *in situ* and on the fly. Perhaps our greatest challenge will be to assess our ability to deal with various types of attacks on our systems while ensuring that vital operations are not harmed or degraded.

We also need measures that reflect more than system performance or indeed the performance of a federation of systems. We need to be able to assess all of the links in the NCW value chain. But the transformation of test and evaluation will be about more than what is measured and how it is measured; it will also be about how test and evaluation activities relate to the organizations and processes that develop new concepts and co-evolve mission capability packages.

Central to this co-evolution process is experimentation. One cannot say, in advance, exactly what level of performance is needed, nor identify the consequences associated with higher or lower levels of performance. Hence, it makes no sense to try to establish pass/fail standards in advance. In fact, it is just these things that concept-based experimentation is supposed to determine. The partnership growing between developers and operators in experimental settings needs to extend to the test and evaluation community as well. We need to work toward achieving a process in which all of the participants lend their expertise and experience to innovate, and then to refine and improve, a capability over time.

There is an imperfect, yet telling, analogy that can be drawn involving the changes that have taken place in the business world between producers and suppliers. Once there existed an arm's-length, almost adversarial, relationship between producers and suppliers. Neither would share information with one another for fear that it would be used against them. Today, producers and suppliers can be seen working closely together to achieve greater levels of quality and efficiency. Suppliers now have a much better idea of what the producers need, and producers now better understand what it takes to supply them with what they need. The net result has been greater stability, dramatic improvements in cost structures and higher quality, with, as a result, improved value to customers and more profit all around. A closer working relationship between the test and evaluation and the operational and technical communities promises analogous gains.

The command, control, communications, computers, intelligence, surveillance and reconnaissance (C⁴ISR) and test and evaluation challenges associated with DoD transformation are formidable. I look forward to working with the test and evaluation community to develop the metrics, instruments, methods, environments, tools and processes needed to adequately test and evaluate information-age technologies, systems and concepts. ❏

The Honorable John P. Stenbit became the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) on August 7, 2001. Prior to this appointment, his private and public sector service in the telecommunications and command and control (C²) fields has spanned more than 30 years. From 1973-1977, he served in the Department of Defense for four years, two of which were spent as principal deputy director of telecommunications and C² systems. The other two years, he served as staff specialist for Worldwide Military Command and Control Systems in the Office of the Secretary of Defense. In 1968, Stenbit joined TRW and was responsible for the planning and analysis of advanced satellite surveillance systems. He retired as an executive vice president of TRW in 2001. Before joining TRW, he was with the Aerospace Corporation, where he worked on C² systems for missiles and satellites and on satellite data compression and pattern recognition. During this time, he studied and taught for two years as a Fulbright Fellow and then as an Aerospace Corporation fellow at the Technische Hogeschool, Einhoven, Netherlands, concentrating on coding theory and data compression. Previously, Stenbit has served as chairman of the Science and Technology Advisory Panel to the director of Central Intelligence and was a member of the Science Advisory Group to the directors of Naval Intelligence and the Defense Communications Agency. He also chaired the Research, Engineering and Development Advisory Committee for the administrator of the Federal Aviation Administration and has served on the Defense Science Board, the Navy Studies Board and the National Research Council manufacturing board. In 1999, he was inducted into the National Academy of Engineering. He received a bachelor's degree and a master's degree in electrical engineering from the California Institute of Technology. He is a member of Tau Beta Pi, the engineering honorary society.

Endnote

[1] Opening line of the Executive Summary of the Network Centric Warfare Report to Congress, which can be found at on the web at *www.c3i.osd.mil/NCW*